## IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

| | |
|---|---|
| In re Application of: | Ashley, Paul Anthony |
| Serial Number: | 10/621,935 |
| Filing Date: | July 17, 2003 |
| Art Unit: | 2432 |
| Examiner: | Dinh, Minh |
| For: | **Method and system for automatic adjustment of entitlements in a distributed data processing environment** |

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

## APPEAL BRIEF

This Brief is submitted pursuant to 37 CFR 41.37.

(i) Real Party In Interest. The real party in interest on this appeal is International Business Machines Corporation ("IBM"), the assignee of record.

(ii) Related Appeals and Interferences. There are no prior and pending appeals, judicial proceedings or interferences known to the appellant that may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

(iii) Status of Claims. The status of all the claims in the application is set forth in the following claim listing. Each of claims 1-3, 5, 7-10, 12, 14-17, 19 and 21-27 is on appeal.

1. (rejected)
2. (rejected)
3. (rejected)
4. (cancelled)
5. (rejected)
6. (cancelled)
7. (rejected)
8. (rejected)
9. (rejected)
10. (rejected)
11. (cancelled)
12. (rejected)
13. (cancelled)
14. (rejected)
15. (rejected)
16. (rejected)
17. (rejected)
18. (cancelled)
19. (rejected)
20. (cancelled)

21. (rejected)

22. (rejected)

23. (rejected)

24. (rejected)

25. (rejected)

26. (rejected)

27. (rejected)

(iv) Status of Amendments.

There are no un-entered amendments.

(v) Summary of Claimed Subject Matter.

The following is a concise explanation of the subject matter defined in each of the independent claims that are the subject of the appeal.

Claim 1 describes a method for restricting access to a set of physical resources in a distributed data processing system. The method begins in response to receipt from a user of a request to access one of the set of physical resources (FIG. 4A, step 402, page 19, lines 21-23). A set of authorized resources for which the user is authorized to access is then determined (FIG. 4A, step 406, page 19, line 31 through page 20, line 4; FIG. 4B, steps 452-454, page 20, line 26 through page 21, line 9). The set of authorized resources is a subset of the set of physical resources. The method then continues by an entitlement server (FIG 2, element 206; page 16, lines 12-15, page 19, line 15 though page 20, line 4, and page 20, line 19 thorough page 23, line; Figure 4B; element 500, FIG. 5 and associated text) obtaining state information about the set of authorized resources. The entitlement server then evaluates availability of the set of authorized resources by comparing the state information about the set of authorized resources against a configurable rule associated with one or more resources in the set of authorized resources (FIG. 4B, steps 460, 462; page 21, lines 22-28). In response to evaluating availability of the set of authorized resources using the configurable rule, the entitlement server then generates a list of a set of entitled resources for the user (FIG. 4A, step 408; page 20, lines 5-10; FIG. 4B, steps 464, 466 and 468, page 21, line 29 through page 22, line 12). The set of entitled resources is a subset of the set of authorized resources. The user is then prevented from accessing physical resources that are in the set of authorized resources but that are not in the set of entitled resources (page 20, lines 5-18; page 23, lines 4-17).

Claim 9 describes an apparatus for restricting access to a set of physical resources in a distributed data processing system. The apparatus comprises a processor (FIG. 1B, element 122), and a computer memory (FIG. 1B, elements 124, 126 and 132) holding computer program instructions (page 29, line 6) which when executed by the processor perform a method. The method begins in response to receipt from a user of a request to access one of the set of physical resources (FIG. 4A, step 402, page 19, lines 21-23). A set of authorized resources for which the user is authorized to access is then determined (FIG. 4A, step 406, page 19, line 31 through page 20, line 4; FIG. 4B, steps 452-454, page 20, line 26 through page 21, line 9). The set of authorized resources is a subset of the set of physical resources. The method then continues by obtaining state information about the set of authorized resources (page 16, lines 12-15, page 19, line 15 though page 20, line 4, and page 20, line 19 thorough page 23, line; Figure 4B; element 500, FIG. 5 and associated text). The availability of the set of authorized resources is then evaluated by comparing the state information about the set of authorized resources against a configurable rule associated with one or more resources in the set of authorized resources (FIG. 4B, steps 460, 462; page 21, lines 22-28). In response to evaluating availability of the set of authorized resources using the configurable rule, a list of a set of entitled resources for the user is then generated (FIG. 4A, step 408; page 20, lines 5-10; FIG. 4B, steps 464, 466 and 468, page 21, line 29 through page 22, line 12). The set of entitled resources is a subset of the set of authorized resources. The user is then prevented from accessing physical resources that are in the set of authorized resources but that are not in the set of entitled resources (page 20, lines 5-

18; page 23, lines 4-17).

Claim 15 describes a computer program product in a computer readable medium (page 29, lines 1-13, as amended) for use in a distributed data processing system (FIG. 1A, and associated text) for restricting access to a set of physical resources. The computer program product holds computer program instructions (page 29, line 6) which when executed by the distributed data processing system perform a method. The method begins in response to receipt from a user of a request to access one of the set of physical resources (FIG. 4A, step 402, page 19, lines 21-23). A set of authorized resources for which the user is authorized to access is then determined (FIG. 4A, step 406, page 19, line 31 through page 20, line 4; FIG. 4B, steps 452-454, page 20, line 26 through page 21, line 9). The set of authorized resources is a subset of the set of physical resources. The method then continues by obtaining state information about the set of authorized resources (page 16, lines 12-15, page 19, line 15 though page 20, line 4, and page 20, line 19 thorough page 23, line; Figure 4B; element 500, FIG. 5 and associated text). The availability of the set of authorized resources is then evaluated by comparing the state information about the set of authorized resources against a configurable rule associated with one or more resources in the set of authorized resources (FIG. 4B, steps 460, 462; page 21, lines 22-28). In response to evaluating availability of the set of authorized resources using the configurable rule, a list of a set of entitled resources for the user is then generated (FIG. 4A, step 408; page 20, lines 5-10; FIG. 4B, steps 464, 466 and 468, page 21, line 29 through page 22, line 12). The set of entitled resources is a subset of the set of authorized resources. The user is then prevented from accessing physical resources that are in the set of authorized resources but that are not in the set of entitled resources (page 20, lines 5-18; page 23, lines 4-17).

Means-plus-function (MPF) structure

There are no MPF-style claim limitations in the pending claims.

(vi) Grounds of Rejection to be Reviewed on Appeal

Group I – claims 1, 3, 5, 7-8, 10, 12, 14-15, 17, 19 and 21

Whether the Examiner erred in finding that Kilkkilä, U.S. Patent No. 6,854,060 ("Kilkkila"), in view of Burke et al, "Simulation In A Distributed Mobile Switching Center Environment ("Burke"), and further in view of Garg et al, U.S. Patent No. 7,434,257 ("Garg"), is the subject matter, taken as a whole, of any of claims 1, 3, 5, 7-8, 10, 12, 14-15, 17, 19 and 21?

Group II – claims 2, 9 and 16

Whether the Examiner erred in finding that Kilkkila in view of Burke, and further in view of Garg, is the subject matter, taken as a whole, of any of claims 2, 9 and 16?

Group III – claims 22-27

Whether the Examiner erred in finding that Kilkkila in view of Burke, and further in view of Garg, is the subject matter, taken as a whole, of any of claims 22-27?

(vii) Argument.

"[A]n applicant can overcome a [Section 103] rejection by showing insufficient evidence of *prima facie* obviousness or by rebutting the *prima facie* case, ..." *See*, *In re Kahn*, 441 F.3d 977, 985-86 (Fed. Cir. 2006). In considering this question, it is appropriate to consider whether the Examiner has met his or her burden to show that the claimed subject matter is disclosed "clearly and unequivocally" in a cited reference. *In re Arkley*, 455 F.2d 586, 587 (CCPA 1972). This issue is evaluated from the viewpoint of a person of ordinary skill in the art, who is a person of ordinary creativity, not an automaton. *KSR Int'l Co. v. Teleflex, Inc.*, 550 U.S. 398, 421, 127 S.Ct. 1727 (2007).

Whether or not particular subject matter "as a whole" would have been obvious to one of ordinary skill in the art at the time an invention was made depends on underlying factual inquiries including: (1) the scope and content of the prior art; (2) the level of ordinary skill in the art; and (3) the differences between the prior art and the claimed invention. *Graham v. John Deere Co.*, 383 U.S. 1, 17 (1966). In rejecting claims under 35 U.S.C. §103(a), it is incumbent upon the Examiner to establish a factual basis to support the legal conclusion of obviousness. *See*, *In re Fine*, 837 F.2d 1071, 1073 (Fed. Cir. 1988).

Rejections based on §103 must rest on a factual basis with these facts being interpreted without hindsight reconstruction of the invention from the prior art. The Examiner may not "resort to speculation, unfounded assumptions or hindsight reconstruction to supply deficiencies in its factual basis." *In re Warner*, 379 F.2d 10100, 1017 (CCPA 1967), *cert. denied*, 389 U.S. 1057 (1968). The key to supporting any *prima facie* conclusion of obviousness under 35 U.S.C. §103(a) is the clear articulation of the reason(s) why the claimed invention would have been obvious. The Court in *KSR* noted that the analysis supporting a rejection should be explicit: "rejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness." *In re Kahn*, 441 F.3d 977, 988 (Fed. Cir. 2006), cited with approval in *KSR*, 550 U.S. at 418.

In considering grounds of rejection, "every limitation in the claim must be given effect rather than considering one in isolation from the others." See, *In re Geerdes*, 491 F. 2d 1260, 1262-63 (CCPA 1974). Moreover, a rejection based on prior art cannot be based on speculations and assumptions. *In re Steele*, 305 F. 2d 859, 862 (CCPA 1962). Further, every limitation in a claim is material to patentability. (*See*, 35 U.S.C. §103(a) concerning the subject matter "as a whole").

An invention "composed of several elements is not proved obvious merely by demonstrating that each of its elements was, independently, known in the prior art. . . . [I]t can be important to identify a reason that would have prompted a person of ordinary skill in the relevant field to combine the elements in the way the claimed new invention does." *KSR Int'l Co. v. Teleflex Inc.*, 550 U.S. 398, 418 (2007).

Group I – claims 1, 3, 5, 7-8, 10, 12, 14-15, 17, 19 and 21

The Scope and Content of the Cited Art

A determination regarding alleged obviousness under 35 USC §103(a) requires an analysis of the "scope and content" of the cited art.

Kilkkila teaches defining a set of commands or a set of terminals that are operated by a set of commands and then restricting the command set upon one or more events or occurrences.

The command set is included in an "access right profile" and, as indicated in FIG. 2 at step 21, that "profile" may be changed (by modifying the command set) when "a predetermined situation occurs in the operation of the telephone switching system."

Kilkkila describes two embodiments of the "access right profile," one relating to "users" and the other relating to "terminals." (See, column 1, lines 37-39; column 4, line 66 – column 5, line 1). A terminal as used in the patent is some form of management interface device for managing or controlling some operation of the telephone switching system. In this system, apparently a user can use a terminal and enter one or more control commands via a command line interface to control some aspect of the telephone switching system operation.

In the case of an "access right profile" in a first embodiment, that profile includes "which MML (Man Machine Language) command language commands the user is authorized to execute." (See, column 1, lines 39-42). According to the described system, upon a particular occurrence (e.g., a time of day, a utilization rate, a predetermined alarm, a session duration, a type of command used, or number of sessions held), the profile is modified, in this embodiment to remove or limit the "commands" the user is authorized to execute. (See, column 4, lines 33-45).

In the case of an "access right profile" in a second embodiment, that profile "pertains to a given set of terminals" and defines "the circumstance that sessions relating to the management of the computer system or telephone switching system can only be activated from a given terminal on certain conditions. (See, column 1, lines 47-51). Upon a particular occurrence, in this embodiment the system apparently restricts or limits what a particular user can do on a particular terminal identified in the profile. (See, column 4, lines 54-62). Once again, this is a limitation of the "commands" themselves.

Burke

Burke describes utilizing phone switching systems in a "distributed" environment (Abstract).

Garg

Garg describes a system and method for incorporating dynamic factors into decisions to provide access to applications, services and objects in computer system. (C3L26-31) The dynamic factors include dynamic groups (assigning temporary group membership based on transient or changing factors) and dynamic access check (based on transient or changing factors such as data from client operations). Dynamic data, such as client operation parameter values, client attributes stored in a time-varying or updateable data store, run-time or environmental factors such as time-of-day, and any other static or dynamic data that is managed or retrievable by the application, may be evaluated in connection with access control decisions.

In Garg, a dynamic authorization "callback mechanism" implements this functionality. FIGS 5A-5C illustrates an embodiment. Referring to FIG. 5A, at application start up, at step 500, the application initializes a resource manager and at step 510, the application registers with the resource manager ComputeDynamicGroups and DynamicAccessCheck callback functions. At step 515, when a client request for an object or property is received, at 520, the application initializes a client context for that client using one or more of the client context initialization routines. If the application possesses information, such as system data, environment data, additional client attributes or client parameter values passed in from client operation that must be evaluated to determine whether the client should be made a member of dynamic groups, the application passes this information into the utilized client context initialization routine(s). Within the client context initialization routine(s) performed at 520, the resource manager first populates the client context with a user identifier and a group identifier associated with the system-level client context passed into the routine. Then, at step 530, the resource manager invokes the ComputeDynamicGroups callback function, if present, passing the relevant dynamic data of the client context initialization routine(s) into one or more argument parameters. Within the application code that implements ComputeDynamicGroups, the application evaluates the client context, its argument parameter(s), and any flexible authorization policy defined in code or a separate store. Based on this evaluation, the application may identify, and return, one or more dynamic groups to which the client should be assigned. At step 540, these dynamic groups are then added to the list of user and group identifiers in the client context. (C10L47 through C11L38)

Thus, the above-described mechanism teaches dynamic computation of a client context when a client request for an object is received (step 515).

Level of Ordinary Skill

The record does not include independent evidence of the level of ordinary skill in the art. Thus, the skill level may be inferred from the references. *In re GPAC*, 57 F.3d 1573, 1579 (Fed. Cir. 1995).

Differences Between The Claims and the Cited Art

Turning to the “differences” between the cited art and the claims, the Examiner contends (Final Rejection at 2-3) that Kilkkila teaches all of the subject matter of each independent claim except for the "distributed" nature of the environment and that the set of authorized resources is determined "in response to receipt from a user of a request to access one of [a] set of physical resources." The Applicant concurs with the Examiner's conclusion in this regard (regarding the claim teachings that are absent from Kilkkila), however, the base conclusion (what claim elements Kilkkila does teach) are overstated.

As described, an "access right profile" in Kilkkila is the only construct in the patent that is modified as a result of the predetermined situation that occurs "in the operation of" the telephone system. (Kilkkila does not disclose or suggest any embodiment that restricts access to the management terminal itself).

With respect to the first Kilkkila embodiment (where the access right profile consists of just a set of commands that may be performed by a user), this embodiment does not reach certain aspects of the claim language. In particular, because the construct that is being modified in Kilkkila is the "access right profile" data, the Examiner must be interpreting the "authorized resources" limitation as the set of commands that are available in the unmodified profile. According to the claim, however, "state information about the set of authorized resources" is then obtained and evaluated so that this set can be pruned down to a set of "entitled resources" that the user is then permitted to access. In the case of first Kilkkila embodiment, the system there is not obtaining "state information" about the "commands" listed in the access right profile and then pruning that command list to a "set of entitled [commands]." Rather, in Killkila (the first embodiment), the system has a set of commands in the access right profile that are modified according to other factors – but not the "state information about the set of authorized resources."

In other words, if the "authorized resources" equate to the data (the list of commands) in the access right profile, then the claim language is not met.

Regarding the Kilkkila second embodiment, the outcome is no different if the "access right profile" consists of a set of terminals. While it is true that a set of terminals is a "set of physical resources," the claims (such as representative claim 1) include still other limitations that are not met by the embodiment. In particular, claim 1 further requires that the state information be evaluated to generate the pruned list (the "entitled resources"), but then the claim goes on to require "preventing the user from accessing resources that are in the set of authorized resources but that are not in the set of entitled resources." In this second embodiment, the occurrence of the condition that triggers the access right profile modification does not limit access to the management terminal; rather, the system only appears to restrict or limit a user's ability to enter/execute certain commands from that terminal. Stated another way, access to the physical resource – the terminal – is not restricted. Thus, the other claim requirement of "preventing the user from accessing resources [the "resources" this time being the terminals identified in the profile]" is not met in this second embodiment either.

Kilkkila teaches defining a set of commands or a set of terminals that are operated by a set of commands and then restricting the command set upon one or more events or occurrences. Despite the similarities in nomenclature, the disclosed method, apparatus and computer program product here address a different problem – "restricting access to a set of physical resources in a distributed data processing system" where a physical resource is a resource for which access (by a user) is controlled or restricted. In Kilkkila, and because the only entity being modified is the "access right profile," Kilkkila is simply "restricting access" to a set of commands in a management interface. While the effect of that restriction might also be to limit some function or operation of the telephone switching system, the particular manner as to how this system restriction is done is not what is being claimed here.

Burke is cited solely for its use of a distributed operating environment. (Final Rejection, at page 4)

Garg is cited as a method for providing dynamic authorization "[such as based on time of day] wherein a user access right profile (i.e. client context) is modified only when the corresponding user requests [access to a resource]." (Final Rejection, at page 4) With respect, the Examiner's finding in this regard is an overstatement. The portions of the Garg specification relied upon by the Examiner merely indicate that the "client context" is dynamically computed in response to receiving the client request. Figure 4 illustrates the client context as including a user identifier 422, a group identifier 422, and an identifier 426 for a dynamic group to which the client should be assigned. The Garg teaches building this "context" not taking some larger set of entries and then pruning.

Moreover, the Examiner's use of Garg for the "in response to" phrase has decoupled this phrase from the rest of the claim phrase, which in its entirety reads as follows:

"in response to receipt from a user of a request to access one of the set of physical resources, determining a set of authorized resources for which the user is authorized to access, wherein the set of authorized resources is a subset of the set of physical resources."

Garg simply builds a client context in response to a client request; the "in response to" phrase in the claim triggers a different action – namely, "determining a set of authorized resources for which the user is authorized to access, wherein the set of authorized resources is a subset of the set of physical resources." Garg does not disclose this particular cause and effect relationship.

When alleged obviousness is based on a combination, the appropriate test is what the combined teachings of the references would have suggested to those of ordinary skill in the art. *In re Keller*, 642 F.2d 413, 426 (CCPA 1981). Here, the combined teachings of Kilkkila, Burke and Garg describe an access control method for a distributed system (Burke) having a set of commands or a set of terminals are operated by a set of commands (Kilkkila), and wherein the method responds to a client request (Garg) to restrict the command set upon one or more events or occurrences (Kilkkila). The claimed invention, however, includes additional subject matter as set forth below (emphasis supplied):

Claim 1:

"in response to receipt from a user of a request to access one of the set of physical resources, determining a set of authorized resources for which the user is authorized to access, wherein the set of authorized resources is a subset of the set of physical resources;

obtaining, by an entitlement server, state information about the set of authorized resources;

evaluating availability of the set of authorized resources by the entitlement server comparing the state information about the set of authorized resources against a configurable rule associated with one or more resources in the set of authorized resources;

in response to evaluating availability of the set of authorized resources using the configurable rule, generating, by the entitlement server, a list of a set of entitled resources for the user, wherein the set of entitled resources is a subset of the set of authorized resources; and preventing the user from accessing physical resources that are in the set of authorized resources but that are not in the set of entitled resources."

Claims 8 and 11

"in response to receipt from a user of a request to access one of the set of physical resources, determining a set of authorized resources for which ~~a~~ the user is authorized to access, wherein the set of authorized resources is a subset of the set of physical resources;

obtaining state information about the set of authorized resources;

evaluating availability of the set of authorized resources by comparing the state information about the set of authorized resources against a configurable rule associated with one or more resources in the set of authorized resources;

generating a list of a set of entitled resources for the user in response to evaluating availability of the set of authorized resources, wherein the set of entitled resources is a subset of the set of authorized resources; and

preventing the user from accessing physical resources that are in the set of authorized resources but that are not in the set of entitled resources."

A *prima facie* case of obviousness must be shown with respect to the subject matter "as a whole." See, 35 USC §103(a). The identified subject matter is not present in the combined teachings. For the above reasons, the Examiner's Final Rejection with respect to the claims in Group I should be **REVERSED**.

Group II – claims 2, 9 and 16

Dependent claims 2, 9 and 16 are each separately patentable because, in addition to not generating a list of entitled resources, Kilkkila not disclose or suggest "sending an indication of the set of entitled resources to the user." Figure 5B illustrates an embodiment of this feature.

In rejecting these claims, the Examiner cites to Kilkkila at column 4, lines 2-62. This citation, with respect, is inapposite. The portions identified by the Examiner concern merely how the access right profile is modified (and the effect of such modification). The claim language, however, is more specific – "sending an indication .. to the user." The Examiner has not shown where this particular function is found in Kilkkila (it is not). As noted above, in considering grounds of rejection, "every limitation in the claim must be given effect rather than considering one in isolation from the others." See, *In re Geerdes*, 491 F. 2d 1260, 1262-63 (CCPA 1974). Moreover, a rejection based on prior art cannot be based on speculations and assumptions. *In re Steele*, 305 F. 2d 859, 862 (CCPA 1962). Further, every limitation in a claim is material to patentability. (*See*, 35 U.S.C. §103(a) concerning the subject matter "as a whole").

The Examiner's argument here appears to be that a modification to the access right profile will necessarily be "indicated" when the user then attempts to take some later action; in other words, that the "indication" may be implied. With respect, any such interpretation would be an overbroad and impermissible interpretation of the "indication" wording given the specification (e.g., Figure 5B and associated text). Moreover, the recited indication that is sent to the user is "of the set of entitled resources." As noted above, Kilkkila simply teaches defining a set of commands or a set of terminals that are operated by a set of commands and then restricting the command set; even if (as the Examiner now argues) the user thereafter receives an implied "indication" of this occurrence, the indication is not "of the set of entitled resources."

For the above reasons, the Examiner's Final Rejection with respect to the claims in Group II should be **REVERSED**.

Group III – claims 22-27

Dependent claims 22-27 are rejected under 35 USC §103(a) as being unpatentable over Kilkkila/Burke as applied above, further in view of U.S. Publication No. 2002/0161733 to Grainger. The scope and content of Kilkkila and Burke have been described above.

Grainger describes an automated client server-based IP (intellectual property) data processing system for managing documents relating to drafting and filing of a U.S. patent application. The publication has been cited for the teachings in [0052]-[0054]. Paragraph [0052] describes a set-up process, wherein users are assigned roles that play a part in the workflow. Rules are established that dictate to whom documents are routed at each stage in the process, how often users should be reminded of a task, and what task is required next after each preceding task. IP data processing system 100 has a mechanism for notifying users of required tasks, and for users to notify the system that tasks are complete. The system makes available (for example, through html links to documents stored in database 106) to the appropriate users any documents necessary for performing the relevant task (e.g., a maintenance fee due date reminder task sent to an appropriate in-house practitioner at a technology developer 110(x) may include an html link to the allowed patent so the practitioner can quickly review the patent's abstract and claims). As described in paragraph [0053], once a customer (e.g., technology developer 110, patent law firm 120, etc.) has set-up the IP data processing system to their requirements, the functions available to a particular client system of a particular customer depend on the role of the client system in the patent process. For example, some of the functions provided through Web pages 104 are restricted to only certain individuals and thus may not be accessible to others. Thus, Web pages 104 include different "home" pages that are the initial Web pages displayed to a client system based upon the role of the client system in the patent process. These home pages include html links to functions that have been determined to be appropriate for the particular client system as part of the set-up procedure. Paragraph [0054] describes an example where the home page that is presented to the client system for an inventor working at a particular technology developer 110(x) is different from the home page that is presented to an in-house practitioner working at the same technology developer 110(x).

Claims 22, 24 and 26 recite that the set of resources are identified by Uniform Resource Identifiers (e.g., URLs), and further that the "preventing" function provides the user a web page without a particular URI for an authorized but non-entitled resource. In Grainger, the functions available to a particular client system of a particular customer depend on the role of the client system in the patent process, and the functions provided through Web pages 104 displayed to a client system are based upon the role of the client system in the patent process and as determined "as part of the set-up procedure." The claim language, however, is more specific; the URI for "an authorized [but non-entitled] resource" is not provided in the web page; in Kilkkila/Burke/Grainger, at most the access right profile command set would be modified but "based upon the role of the client system" and "as part of the set-up procedure" i.e., not "in response to" an access request that is for an "authorized [but non-]entitled resource."

Dependent claims 23, 25 and 27 recite that the set of resources may include a resource that one user (having a given status) may be entitled to access while another user (not having the given status) may not be entitled to access (even though, e.g., the same resource is otherwise available). These claims are likewise patentable for the same reasons advanced with respect to claims 22, 24 and 26. The Kilkkila/Burke/Grainger combination would not function "in response to" an access request that is for an "authorized [but non-]entitled resource."

For the above reasons, the Examiner's Final Rejection with respect to the Group III claims should be **REVERSED**.

Respectfully submitted,

By: /David H. Judson/

David H. Judson, Reg. No. 30,467

ATTORNEYS FOR APPLICANT

April 23, 2010

1. A method for restricting access to a set of physical resources in a distributed data processing system, the method comprising:

in response to receipt from a user of a request to access one of the set of physical resources, determining a set of authorized resources for which the user is authorized to access, wherein the set of authorized resources is a subset of the set of physical resources;

obtaining, by an entitlement server, state information about the set of authorized resources;

evaluating availability of the set of authorized resources by the entitlement server comparing the state information about the set of authorized resources against a configurable rule associated with one or more resources in the set of authorized resources;

in response to evaluating availability of the set of authorized resources using the configurable rule, generating, by the entitlement server, a list of a set of entitled resources for the user, wherein the set of entitled resources is a subset of the set of authorized resources; and

preventing the user from accessing physical resources that are in the set of authorized resources but that are not in the set of entitled resources.

2. The method of claim 1 further comprising:

sending an indication of the set of entitled resources to the user.

3. The method of claim 1 further comprising:

responding to requests for the user to access the set of entitled resources.

4. (cancelled)

5. The method of claim 1 further comprising:

considering user attributes of the user while evaluating availability of the set of authorized resources.

6. (cancelled)

7. The method of claim 1 further comprising:

gathering state information for the set of resources using a distributed monitoring application.

8. An apparatus for restricting access to a set of physical resources in a distributed data processing system, the apparatus comprising:

a processor;

a computer memory holding computer program instructions which when executed by the processor perform a method comprising:

in response to receipt from a user of a request to access one of the set of physical resources, determining a set of authorized resources for which ~~a~~ the user is authorized to access, wherein the set of authorized resources is a subset of the set of physical resources;

obtaining state information about the set of authorized resources;

evaluating availability of the set of authorized resources by comparing the state information about the set of authorized resources against a configurable rule associated with one or more resources in the set of authorized resources;

generating a list of a set of entitled resources for the user in response to evaluating availability of the set of authorized resources, wherein the set of entitled resources is a subset of the set of authorized resources; and

preventing the user from accessing physical resources that are in the set of authorized resources but that are not in the set of entitled resources.

9. The apparatus of claim 8 wherein the method further comprises:

sending an indication of the set of entitled resources to the user.

10. The apparatus of claim 8 wherein the method further comprises:

responding to requests for the user to access the set of entitled resources.

11. (cancelled)

12. The apparatus of claim 8 wherein the method further comprises:

considering user attributes of the user while evaluating availability of the set of authorized resources.

13. (cancelled)

14. The apparatus of claim 8 wherein the method further comprises:

gathering state information for the set of resources using a distributed monitoring application.

15. A computer program product in a computer readable medium for use in a distributed data processing system for restricting access to a set of physical resources, the computer program product holding computer program instructions which when executed by the distributed data processing system perform a method comprising:

in response to receipt from a user of a request to access one of the set of physical resources, determining a set of authorized resources for which the user is authorized to access, wherein the set of authorized resources is a subset of the set of physical resources;

obtaining state information about the set of authorized resources;

evaluating availability of the set of authorized resources by comparing the state information about the set of authorized resources against a configurable rule associated with one or more resources in the set of authorized resources; and generating a list of a set of entitled resources for the user in response to evaluating availability of the set of authorized resources, wherein the set of entitled resources is a subset of the set of authorized resources; and

preventing the user from accessing physical resources that are in the set of authorized resources but that are not in the set of entitled resources.

16. The computer program product of claim 15 wherein the method further comprises:

sending an indication of the set of entitled resources to the user.

17. The computer program product of claim 15 wherein the method further comprises:

responding to requests for the user to access the set of entitled resources.

18. (cancelled)

19. The computer program product of claim 15 wherein the method further comprises:

considering user attributes of the user while evaluating availability of the set of authorized resources.

20. (cancelled)

21. The computer program product of claim 15 wherein the method further comprises:

gathering state information for the set of resources using a distributed monitoring application.

22. The method as described in claim 1 wherein the set of resources are identified by Uniform Resource Identifiers (URIs), and the step of preventing the user from accessing resources includes providing the user a web page without a URI for an authorized resource that is not also an entitled resource.

23. The method as described in claim 1 wherein the set of entitled resources for the user includes a particular authorized resource that the user is entitled to access as a result of the evaluating step and further as a result of a given user status being met, wherein the particular authorized resource, although included in the set of entitled resources for the user, is omitted from a list of entitled resources for another user that does not then have the given user status.

24. The apparatus as described in claim 8 wherein the set of resources are identified by Uniform Resource Identifiers (URIs), and the step of preventing the user from accessing resources includes providing the user a web page without a URI for an authorized resource that is not also an entitled resource.

25. The apparatus as described in claim 8 wherein the set of entitled resources for the user includes a particular authorized resource that the user is entitled to access as a result of the evaluation and further as a result of a given user status being met, wherein the particular authorized resource, although included in the set of entitled resources for the user, is omitted from a list of entitled resources for another user that does not then have the given user status.

26. The computer program product as described in claim 15 wherein the set of resources are identified by Uniform Resource Identifiers (URIs), and the step of preventing the user from accessing resources includes providing the user a web page without a URI for an authorized resource that is not also an entitled resource.

27. The computer program product as described in claim 15 wherein the set of entitled resources for the user includes a particular authorized resource that the user is entitled to access as a result of the evaluation and further as a result of a given user status being met, wherein the particular authorized resource, although included in the set of entitled resources for the user, is omitted from a list of entitled resources for another user that does not then have the given user status.

(ix) Evidence Appendix.

None.

(x) Related Proceeding Appendix.

None.